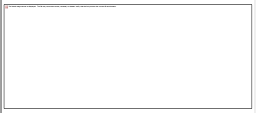
China's Electronic Strategies

by Mr. Timothy L. Thomas, Foreign Military Studies Office, Fort Leavenworth, KS.



The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

This article appeared in

Military Review

May-June 2001

Major General Dai Qingmin, director of the Chinese People's Liberation Army's (PLA's) Communications Department of the General Staff responsible for information warfare (IW) and information operations (IO), wrote that "new technologies are likely to find material expression in informationalized arms and equipment which will, together with information systems, sound, light, electronics, magnetism, heat and so on, turn into a carrier of strategies."[1] Chinese strategies rely on electrons in unanticipated ways to fulfill stratagems such as "kill with a borrowed sword" or "exhaust the enemy at the gate and attack him at your ease."

The Chinese believe that superior strategies can help overcome technological deficiencies. A comparable equivalent to this theoretical development in military art would be a Russian virtual operational maneuver group of electron forces or a US air-land electron battle group.

Dai's article is an important benchmark in PLA military philosophy. First, he is a very credible and responsible figure. Before his present job, Dai commanded the PLA's Information Warfare Center in Wuhan. Second, he defines IW and IO with Chinese characteristics that are different from US definitions. Third, Dai broke tradition and advocated pre-emptive attack to gain the initiative and seize information superiority. This offensive emphasis contradicts China's military strategy of active defense. Finally, he noted that integrated and joint IO gives more scope and purpose to a people's war. Dai's article also indicates that China is clearly developing strategies to implement IW with Chinese characteristics. Other writers support his view with their own approaches to strategic IW.

The journal *China Military Science* is produced by the Academy of Military Science and approximates *Joint Force Quarterly*. It carries articles on a variety of current topics of interest to the PLA, to include information and psychological operations.

> **Major General Dai Qingmin: "Informationized arms . . . together with information systems, sound, light, electronics, magnetism, heat and so on, turn into a carrier of strategies."**

The Fiscal Year 2000 report on China from the US Secretary of Defense to Congress (mandated by the National Defense Authorization Act) indicated growth in Chinese theory and capability. The report noted that since NATO air forces inadvertently bombed the Chinese Embassy in Belgrade on 7 May 1999, Chinese leaders have accelerated military modernization, pursued strategic cooperation with Russia and increased proliferation activities. In particular, China focused on fighting adversaries that had advanced information technologies and long-range precision weapons. The "active-defense" doctrine focuses on "People's War under modern conditions," which the secretary's report termed "local wars under high-tech conditions."[2] Released on 16 October 2000, the Chinese Defense White Paper also emphasized China's people's war tradition, an empha-sis that surprised many Western followers of China who thought the idea had lost relevance in the information age. In fact, its importance has grown.

In September 2000, two weeks before the White Paper was released, the *PLA Daily* released an article on China's military telecommunications (telecom) developments. The article noted that in 1991 Chairman Jiang Zemin called for building common telecom systems for military and civilian use to meet peacetime and wartime needs.[3] Only in such fashion could military telecom catch up with its civilian counterpart. One way to do this was to create reserve forces (a key component uniting civilian and military sectors in a people's war) with telecom and IW/IO missions. The paper noted, "We have built a reserve telecom force structure with a reserve telecom regiment as the backbone, with an information industrial department as the base . . . have built a reserve contingent of qualified high-tech telecom and transmission personnel with those specializing in satellite telecom, relay telecom, digital telecom, telegraph (telephone) telecom, and optical-fiber telecom as the main force . . . and have built a contingent of highly qualified personnel with computer experts, network monitoring experts, as well as radio telecom units serving as the backbone."[4]

China's reserve forces are now being armed with IW/IO missions and have become the high-tech link in the country's people's war theory. In the past, reserve forces' planned role in a people's war was supporting PLA forces defending against foreign intervention. Today's reserve forces can do something even the PLA could not for many years—reach out and touch someone continents away with electronic and information weapons. Properly targeted electronic attacks could be as devastating to a country's economy as damage inflicted by an intercontinental missile.

Civil-military cooperation and integration are growing in China in the information age, just as it is in the United States. Chairman Jiang Zemin (*third from left*) has called for building common telecom systems for military and civilian needs. One way to do this is to create reserve forces—a key component uniting civilian and military sectors in a people's war—with telecom and IW/IO missions.

China's defense industrial complex lags in developing high-technology equipment; therefore, China must find "selective pockets of excellence" according to the late Chinese leader Deng Xiaoping. One of these pockets appears to be internal telecom. The Secretary of Defense's report noted that military and civilian communications networks might be linked to help China in a crisis. The September *PLA Daily* report indicates that a civil-military telecom system is more likely. The military communications system is carried over multiple transmission lines to make it survivable, secure, flexible, mobile and less vulnerable to exploitation, destruction or electronic attack. The command automation data network can reportedly support limited preplanned conventional attack options along China's periphery.[5]

The reserve forces also reportedly have their own websites and simulation centers. China now has 400 military websites, according to one report.[6] On 7 January 2001 several unidentified companies agreed to form the China C-Net Strategic Alliance, a second-generation Internet-like network for China's government and industry. No start dates for construction or completion were offered. The Xinhua News Agency release noted that "the current one [Internet] has too many faults and is incapable of satisfying the needs of the Chinese government and companies as they enter the digital age. It is unknown whether foreigners will have access to the net, or if it will be compatible with the existing net."[7]

IW/IO Strategy in *China Military Science*

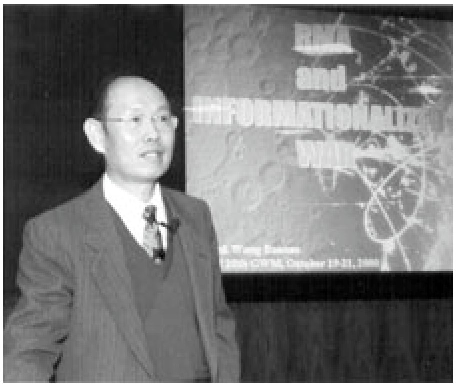
The journal *China Military Science*, which approximates *Joint Force Quarterly*, has provided a limited forum for IW/IO articles over the past year. However, the April 2000 issue was an exception. The journal contains three articles on IO subjects, and all three are important. One article is titled "The Current Revolution in Military Affairs and its Impact on Asia-Pacific

Security," by Senior Colonel Wang Baocun. Wang is a well-respected author on IO subjects and works in the Foreign Military Studies Department of the Academy of Military Science, which publishes *China Military Science*. Wang's article is the only one in the issue in English and reflects a Western view of IW and the Revolution in Military Affairs. For example, Wang defines IW as "a form of combat actions which attacks the information and information systems of the enemy while protecting the information and information systems of one's own side. The contents of IW are military security, military deception, physical attack, electronic warfare, psychological warfare and net warfare, and its basic purpose is to seize and maintain information dominance."[8]

Wang provided a very different definition of IW when writing for the same journal in 1997. His description of IW contained the elements of Soviet/Russian military science, covering the nature, forms, levels, distinctions, features and principles of IW. Wang listed forms of IW as peacetime, crisis and wartime; the nature of IW as reflected in offensive and defensive operations; levels of IW as national, strategic, theater and tactical; and other distinctions of IW as command and control, intelligence, electronic-psychological, cyberspace, hackers, virtual, economics, strategy and precision. He listed features of IW as complexity, limited goals, short duration, less damage, larger battle space and less troop density, transparency, intense struggle for information superiority, increased integration, increased demand on command, new aspects of massing forces and the fact that effective strength may not be the main target. He stated that principles of IW include decapitation, blinding, transparency, quick response and survival.[9]

The two definitions Wang offered reflect two ways of viewing IW in China. The first definition is through the prism of Western theory, and the second is through the prism of Soviet/Russian military science, which was used extensively from the 1950s to the early 1990s. In recent lectures, Wang spoke of "informationalized warfare," a concept Dai used quite often in his article.[10]
;

"On Information Warfare Strategies," by Major General Niu Li, Colonel Li Jiangzhou and Major Xu Dehui at the Communications and Command Institute, appeared in the same April 2000 issue. The authors define IW stratagems as "schemes and methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare."[11] Chinese leaders believe that stratagems to technological inferiority can be achieved by combining human qualitative thinking with computer-assisted quantitative calculations. The authors suggest devising stratagems that are based on cognition and technology (information acquisition and processing).



Senior Colonel Wang Baocun of the PLA's Academy of Military Sciences lecturing at the US Army Command and General Staff College in January 2001 on "Informationalized War," a concept that Major General Dai also addresses.

Asians and Occidentals view combining stratagems with technology differently. The authors note that, "Traditionally, Oriental people emphasize stratagems and Occidental people emphasize technology . . . Occidental soldiers would seek technological means when encountering a difficulty, while Oriental soldiers would seek to use stratagems to make up for technological deficiencies without changing the technological conditions. Oriental soldiers' traditional way of thinking is not conducive to technological development, but can still serve as an effective way of seeking survival in a situation of danger."[12] IW stratagems can:

- Direct commanders' thinking and force them to make errors by attacking cognitive and belief systems.
- Generate heavy psychological pressure by using intimidation to signal inevitable victory concentrating forces and coordinating information networks.
- Intimidate by demonstrating capabilities.
- Adopt active and effective measures to generate surprise, and use decisive technical equipment and IW means.
- Develop and hide IW "killer weapons."
- Hide reality by creating a fictitious reality.
- Apply deceptive schemes simultaneously or consecutively.
- Use all IW means to maintain supremacy.
- Mislead the enemy by pretending to follow his wishes.
- Release viruses to contaminate information flows.
- Control time elements by conducting information "inducement," deception," "concealment" and "containment."[13]

These strategies are designed to force cognitive errors in the enemy and create a multidimensional threat with which the enemy must contend.

Dai on Information Operation Strategies and a People's War

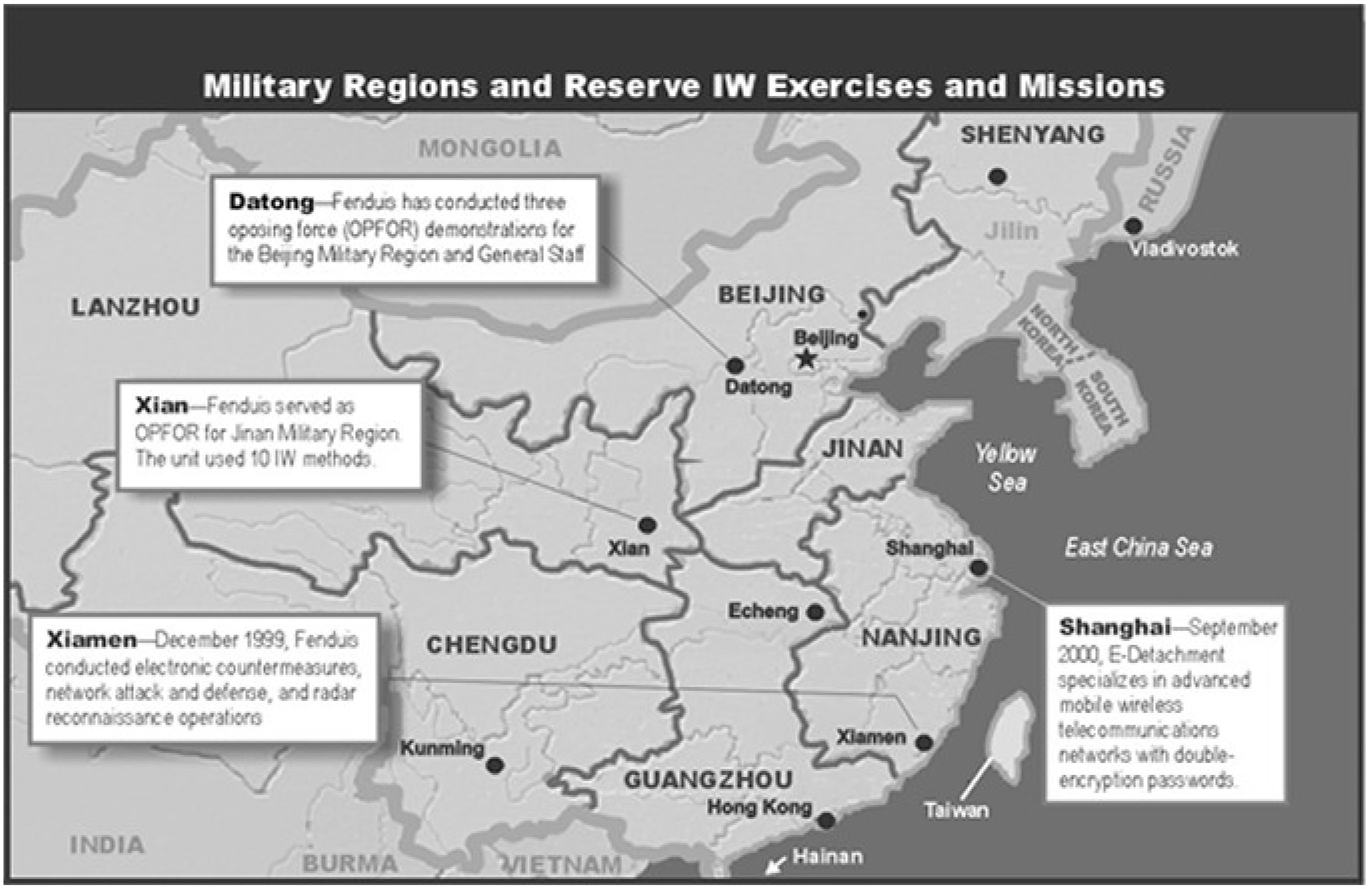
A third article in the April 2000 issue is Dai's "Innovating and Developing Views on Information Operations." Dai defines an information operation as "a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational target, and with electronic warfare and a computer network war as the principal form."[14] Since these operations are trials of strength focusing on knowledge and strategies, Dai recommends a "focus on strategies."

Scientific and technological developments have given strategies a new playing field. A strategy may carry different contents under different technological conditions, allowing room for traditional strategies, and new ones mapped out by new technological means. Options include new information-confrontation strategies, adding strategic wings to technology or applying strategies in light of technology.[15] If technology finds expression in arms and equipment, then information systems and even electrons can be strategy carriers. A good strategy can "serve as a type of invisible fighting capacity; may make up inadequate material conditions to a certain extent; may narrow a technological or equipment gap between an army and its enemy; and may make up for a shortage of information, fighting forces or poor information operational means."[16] Some of these strategies include:

- Jamming or sabotaging an enemy's information or information system.
- Sabotaging an enemy's overall information operational structure.
- Weakening an enemy's information fighting capacity.
- Dispersing enemy forces, arms and fires while concentrating its own forces, arms and fire.
- Confusing or diverting an enemy and creating an excellent combat opportunity for itself.
- Diverting an enemy's reconnaissance attempt and making sufficient preparations for itself.
- Giving an enemy a false impression and launching a surprise information attack on him at the same time.
- Blinding or deafening an enemy with false impressions.
- Confusing an enemy or disrupting his thinking.
- Making an enemy believe that what is true is false and what is false is true.
- Causing an enemy to make a wrong judgment or take wrong action.[17]

Dai also emphasizes that future operations must be integrated. One such concept will be integrating military and civilian information fighting forces. Dai believes that information systems offer more modes for people to take part in IO and serve as a major aux-iliary information fighting force in a future information war.[18] Integrating civilian and military specialists will breathe new life into Mao Zedong's theory of people's war. Chinese IW specialist General Wang Pufeng first noted this condition in 1995.[19]

Ideas for uniting a people's war with IW are finding fertile ground in China's 1.5-million reserve force. Several IW reserve forces have already been formed in the cities of Datong, Xiamen, Shanghai, Echeng and Xian. Each is developing its own specialty as well. For example, Shanghai reserve forces focus on wireless telecom networks and double-encryption passwords.



Military Regions and Reserve IW Exercises and Missions

Datong—Fenduis has conducted three opposing force (OPFOR) demonstrations for the Beijing Military Region and General Staff

Xian—Fenduis served as OPFOR for Jinan Military Region. The unit used 10 IW methods.

Xiamen—December 1999, Fenduis conducted electronic countermeasures, network attack and defense, and radar reconnaissance operations

Shanghai—September 2000, E-Detachment specializes in advanced mobile wireless telecommunications networks with double-encryption passwords.

In Xian, the People's Armed Forces Department reportedly is working with several strategies that resemble Dai's idea of turning light, sound and electronics into strategy carriers. IW Fenduis (divisions) acted as opposing forces for a military district exercise in Jilin Province (Shenyang Military Region). Ten IO methods, which could also be considered as electronic strategies, follow:

- Planting information mines.
- Conducting information reconnaissance.
- Changing network data.
- Releasing information bombs.
- Dumping information garbage.
- Disseminating propaganda.
- Applying information deception.
- Releasing clone information.
- Organizing information defense.
- Establishing network spy stations.[20]

Whether these strategies are used in external reconnaissance of foreign operating systems today is unknown.

A third, significant way the information age has affected China's attitude toward warfare is that China's 36 stratagems may find new meaning and application. Some 300 years ago an unknown scholar decided to collect and record China's stratagems. *The Thirty-Six Stratagems: The Secret Art of War* emphasizes deception as a military art that can achieve military objectives.[21] In the information age, which is characterized by anonymous attacks and uncertainty, the stratagem just might be revitalized as a tactic. It should be easier to deceive or inflict perception-management injuries (guidance injuries in Chinese) as a result. The information age is developing into the anonymous persuaders' age.

Some argue that in today's high-tech world, these ancient stratagems no longer apply. However, a look at just the first five stratagems shows otherwise. Strategy one is "fool the emperor to cross the sea."[22] Lowering an enemy's guard must be an open act, hiding true intentions under the guise of everyday activities. An IW application would be using regular e-mail services or Internet business links to mask insertions of malicious code or viruses. Strategy two is "besiege Wei to rescue Zhao": when the enemy is too strong to attack directly, attack something he holds dear. Today's IW implication is that if you cannot hit someone with nuclear weapons because of catastrophic effects on your own country, then attack the servers and nets responsible for Western financial, power, political and other systems' stability with electrons. Strategy three is "kill with a borrowed sword": when you do not have the means to attack the enemy directly, attack using another's strength. The IW application is simple—send viruses or malicious codes through a cutout or another country.

Strategy four is "await the exhausted enemy at your ease": choosing the time and place for battle is an advantage. Encourage the enemy to expend his energy in futile quests while you conserve your strength. When he is exhausted and confused, attack with energy and purpose. The IW application here is to use the people's war theory to send out multiple attacks while saving the significant attack until all the West's computer emergency response teams (CERTs) are engaged. Finally, strategy five is "loot a burning house": when a country is beset by internal conflicts, it will be unable to deal with an outside threat. The IW application is to put hackers inside the West under the guise of a student or business and attack from the inside. While chaos reigns, steal from information resources.

Integration also implies networking. In the August 2000 newspaper article "PRC Army Pays Attention to the Role of Network Warfare," a people's war received as much attention as networking. The author stated that *Jiefangjun Bao* [the Chinese armed forces newspaper] maintains that it is necessary to formulate rules and regulations regarding mobilization and preparation for "modern People's War," as well as information gathering and processing; online offensives and defense; and network technology research and exchanges, to provide norms for preparing and building a "network People's War."[23]

Attaining information superiority (Dai uses the term 32 times and the concept "information control" 11 times in his article) is crucial to using these strategies in a people's war and requires several steps. First, Dai notes that professional forces (perhaps the PLA) would obtain, transmit and process war information, and jam or sabotage enemy information or information systems. Nonprofessional forces (perhaps the reserves) protect specific targets and injure the enemy's effective fighting strength. Second, electronic warfare means (designed to sabotage information gathering and transmission) and network warfare means (designed to sabotage information processing and use) must be integrated. Third, "soft and hard" are to be used for forces and offensive and defensive operations.[24] The offensive includes electronic, network and other units to destroy enemy electronic systems; and the defense consists of telecom, technical reconnaissance, radar and other units. Fourth, integrated, joint, all-dimensional operations must cover ground, sea, air and space.[25]

Dai remarks that to contend for information superiority requires viewing IO as an "active offensive." This viewpoint appears strongly to contradict the viewpoint expressed in China's subsequent White Paper that stressed China's adherence to an active defense posture. However, Dai notes that for defense to be positive, it must be an "active offensive defense," while a negative information defense will be passive. This word game appears designed to keep the "information active offense" in line with the White Paper.[26] In this sense, Dai recommends the Kosovo model of the Serbs, who actively responded, over the Gulf War model of the Iraqis, who passively waited for the coalition's next step.

Other Information Strategies

A 1996 article notes that information technology is the core and foundation of the military revolution. Information and knowledge have changed the previous practice of measuring military strength, which was calculated by counting the number of armored divisions, air force wings and aircraft carrier battle groups. Invisible forces must be considered in calculating the correlation of forces today. These include:

- Computing capabilities, to include capacity.
- Communications capacity/volume.
- System reliability.
- Ability of reconnaissance systems.[27]

Each element could affect the information strategy employed by or against adversaries. These strategies also possess global reach, speed-of-light transmission and comprehensive integration.

In addition, knowledge and psychological factors must be evaluated as components of the correlation of forces. Knowledge war entails calculating significant changes to people, weaponry and military systems. The impact of a knowledge differential was obvious between US soldiers in the Gulf and Iraq. The high-tech coalition weaponry would have been practically useless to Iraqi soldiers, many of whom were illiterate. Future war, characterized by chessboard-type competition and high-tech knowledge embedded into weapon circuitry, will be "directed by master's degree holders, commanded by university students and conducted by experts." In addition, turning knowledge into weapons will occur more quickly. Networking competence, automation and real-time systems for early warning, reconnaissance, control and guidance, and attack will improve, enabling weapons to identify, differentiate and analyze targets automatically. Military systems will replace quantity and scale with quality and effectiveness.[28] Knowledge war also includes developing superior strategies based on superior knowledge.

The primary conclusion from a review of Chinese IW stratagems is that strategy, the military art and science of conducting campaigns on a broad scale, has undergone a transformation. Concentrations of forces will be replaced by striking efficacy with information and energy, and lines between front and rear will blur. Operations will switch from firepower to detecting, concealing, searching and avoiding, making long-range combat replace hand-to-hand fighting. A core issue will be the fight for network supremacy, which will be necessary to win in strategy and battle simultaneously.

In a revolutionary development, clouds of electrons will be able to disable and destroy countries (usually via economic destruction but also via information-psychological attacks) where once large armies were required. Electrons and information technologies are the new formations of 21st-century armed forces in China and other countries. Electrons in combat require focus on operational effectiveness instead of concentrating military strength. Building systems for soft destruction (signal deception or interference) will become as important as firepower, according to some Chinese analysts. The West should look to the East to explain these stratagems. As the Chinese note, they allow more time for strategic thinking than their Occidental counterparts.

A few new areas of emphasis support these strategies. They include the new criteria for figuring correlation of forces and the new emphasis on cognitive factors, especially psychological. For China, the information revolution has also breathed new life into an old yet timely Chinese strategy—people's war. The country can unite around this concept with its reserve forces and anyone with a laptop computer. For Western audiences, it is time to study these changes closely, and to adapt some into our way of conducting IW.

---

[1] Qingmin Dai, "Innovating and Developing Views on Information Operations," Beijing *Zhongguo Junshi Kexue*, 20 August 2000, 72-77. Translated and downloaded from Foreign Broadcast Information Service (FBIS), 9 November 2000, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

[2] The Report to Congress Pursuant to the FY2000 National Defense Authorization Act, www.defenselink.mil/news/Jun2000/china06222000.htm.

[3] Zhang Fuyou, "With Joint Efforts Made by Army and People, Military Telecommunications Makes Leap Forward," *Beijing Jiefangjun Bao*, September 2000, 9. Translated and downloaded from FBIS, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

[4] Ibid.

[5] The Report to Congress.

[6] Wei Kaqing, "On the Sudden Emergence of Military Websites," Beijing *Zhongguo Guofang Bao*, 6 November 2000, 4. Translated and downloaded from FBIS, 14 December 2000, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

[7] Beijing, *The Associated Press*, 8 January 2001.

[8] Wang Baocun, "The Current Revolution in Military Affairs and its Impact on Asia-Pacific Security," *China Military Science*, April 2000, 139.

[9] Baocun, "A Preliminary Analysis of IW," Beijing *Zhongguo Junshi Kexue*, 20 November 1997, 102-11. Translated and downloaded from FBIS, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

[10] Ibid.

[11] Niu Li, Li Jiangzhou, and Xu Dehui, "On Information Warfare Stratagems," Beijing *Zhongguo Junshi Kexue*, 12 January 2001, 115-22. Translated and downloaded from FBIS, http://sun3.lib/uci.edu/~slca/microform/resources/f-g /f_049.htm.

[12] Ibid.

[13] Ibid.

[14] Dai, "Innovating and Developing Views on Information Operations."

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Wang Pufeng, "Meeting the Challenge of Information Warfare," *Zhongguo Junshi Kexue* (*China Military Science*), 20 February 1995, 8-18. Translated and reported in FBIS-CHI-95-129, 6 July 1995, 29 and 30.

[20] *Xianjin Bao*, 10 December 1999, provided by Mr. William Belk to the author via e-mail.

[21] Wang Xuanming, *The Thirty-Six Strategems: The Secret Art of War* (China Books and Periodicals, December 1992).

[22] These strategies and their meaning were downloaded from http://www.chinastrategies.com; the information-age interpretation is the author's.

[23] "PRC Army Pays Attention to the Role of Network Warfare," Hong Kong *Zhongguo Tonnxun She*, 6 August 2000, translated and downloaded from FBIS, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

24. Dai. "Soft" means temporary sabotage or deception using electronic jamming, computer virus attacks, network infiltration, carbonized-fiber bombs, virtual reality attacks and psychological attacks. "Hard" means permanent sabotage, weakening an enemy's overall fighting capacity, and includes conventional arms, sabotage attacks with forces, attacks with electromagnetic pulses and attacks with arms-carrying direction finders.

25. Ibid.

26. Ibid.

27. Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," *Kuang Chiao Ching*, 16 January 1996, 22 and 23. Translated in FBIS-CHI-96-035, 21 February 1996, 33 and 34.

28. Jia Xi and Shi Hongju, "Analysis on Key Elements of Knowledge Warfare," Beijing *Jiefangjun Bao*,_18 September 2000. Translated and downloaded from FBIS, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

Photos:
People's Liberation Army
US Army